**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF GEORGIA**

| | |
|---|---|
| CHRISTINE PAWESKI, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>ALOGENT HOLDINGS, INC.,<br><br>Defendant. | Case No.: _____<br><br>**COMPLAINT –CLASS ACTION**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Christine Paweski ("Plaintiff"), on behalf of herself and all others similarly situated, brings this Class Action Complaint against Defendant Alogent Holdings, Inc. ("Defendant" or "Alogent"), alleging as follows based upon information and belief, investigation of counsel, and her own personal knowledge.

## NATURE OF THE ACTION

1. Plaintiff brings this class action against Alogent for its failure to properly secure and safeguard personally identifiable information against criminal hackers.

2. Businesses that handle sensitive, personally identifiable information ("PII") owe a duty to the individuals to whom that data relates. This duty to protect PII arises because it is foreseeable that its exposure to unauthorized persons—

especially to hackers with nefarious intentions—will result in harm to the affected individuals.

3. Alogent provides financial digitization and automation services to banks and credit unions. These services include, *inter alia*, facilitating digital check processing for its client financial institutions. As part of its normal business operations, Alogent uses a managed file transfer software called MOVEit.

4. MOVEit software is likewise used by a large number of commercial entities and federal and state agencies to transfer large data files.

5. In order to provide its services, Alogent has access to the financial institutions' account holders' PII, such as their account and routing numbers, names, addresses, phone numbers, check payees and payment amounts, and credit or debit card numbers (as well as a security code, access code, password, or PIN for the account associated with each card).

6. As Alogent is or should have been aware, this type of personal and sensitive data is highly targeted by hackers who seek to exploit that data for nefarious purposes. In the wrong hands, these types of sensitive data may be wielded to cause significant harm to the Class Members.

7. Despite Alogent's duty to safeguard the PII that it processes and collects as part of its business operations, Plaintiff's and Class Members' sensitive information was exposed to unauthorized third parties during a massive data breach

that occurred between May 30, 2023 and June 1, 2023 (the "Data Breach").[1] The Data Breach exploited a vulnerability in the MOVEit technology, which Defendant uses in its regular course of business.

8. The United States Cybersecurity & Infrastructure Security Agency has identified the data exfiltrators as "CL0P Ransomware Gang," also known as TA505, and reports that the attacks were conducted by exploiting a vulnerability catalogued as "CVE-2023-34362" in order to exfiltrate data from the underlying MOVEit databases.[2] CISA reports that TA505 has been known both to publish exfiltrated data and to ransom exfiltrated data for profit.

9. Despite the Data Breach occurring between May 30 and June 1, 2023, Alogent waited until August 14, 2023 to begin notifying consumers that an unauthorized third party had compromised an Alogent server and exposed consumers' PII stored therein.[3]

10. Based on the public statements of Alogent to date, a wide variety of PII was impacted in the Data Breach, including, but not limited to, individuals' names,

---

[1] *Data Breach Notifications – Alogent*, Off. Maine Att'y Gen. (Aug. 29, 2023), https://apps.web.maine.gov/online/aeviewer/ME/40/fa79180f-c61b-4e9a-b2c3-290ceb02e5a2.shtml (last visited Dec. 8, 2023).

[2] *#StopRansomeware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, Cybersecurity & Infrastructure Security Agency (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a (last visited Dec. 8, 2023).

[3] *Id.*

addresses, phone numbers, bank account and routing numbers, and check payees and remittance amounts.[4]

11. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of the exposed PII was due to Alogent's failure to properly secure and safeguard the highly sensitive personal and financial information with which it was entrusted.

12. As a result of the Data Breach, Plaintiff and similarly situated individuals are now at a significantly increased and certainly impending risk of fraud, identity theft, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and similarly situated individuals must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

13. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed and/or compromised during the Data Breach.

14. Plaintiff, on behalf of herself and all others similarly situated, alleges claims for negligence, negligence *per se*, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including the adoption of reasonably sufficient

[4] *Data Breach Notifications – Alogent*, *supra* note 1.

practices to safeguard PII that remains in Alogent's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

## PARTIES

15. Plaintiff Christine Paweski, at all relevant times, is and was a citizen and resident of the State of Michigan. Plaintiff was a customer of one of Alogent's client financial institutions. Plaintiff received a notification from Alogent that her PII was compromised and disclosed without authorization to unknown third parties as a result of the Data Breach.

16. Defendant Alogent Holdings, Inc., is a Delaware corporation with its principal place of business located at 35 Technology Parkway South, Suite 200, Peachtree Corners, Georgia, 30092. Defendant is a citizen of Georgia and Delaware.

## JURISDICTION AND VENUE

17. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

18. This Court has personal jurisdiction over Defendant, as Alogent maintains its principal place of business in Peachtree Corners, Georgia, and, at all

relevant times, Defendant has engaged in substantial business activities in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

## FACTUAL BACKGROUND

### *A. Defendant Provides Technology Services Involving Highly Sensitive Data.*

20. Alogent is a software and services company headquartered in the Atlanta metropolitan area in Georgia.

21. Alogent holds itself out as a "market leader" in providing financial digitization and automation services to banks and credit unions. These services include deposit automation, item processing, digital banking, information management, tracking solutions, and digital check processing.[5]

22. Alogent maintains three offices, employs more than 200 people, and generates approximately $46 million in annual revenue.[6]

---

[5] *Company Overview*, ALOGENT, https://www.alogent.com/company (last visited Dec. 8, 2023).

[6] *Careers*, ALOGENT, https://www.alogent.com/careers (last visited Dec. 8, 2023); *Contact*, ALOGENT, https://www.alogent.com/contact (last visited Dec. 8, 2023); Richard Console, Jr., *Alogent Holdings MOVEit Data Breach Affects Personal Information of Approximately 454,3850*, JD SUPRA (Aug. 30, 2023),

23. Upon information and belief, while administering its services to its financial institution clients, Plaintiff and Class Members are required to directly or indirectly entrust Alogent with their PII. In return, Plaintiff and Class Members reasonably expect that Alogent will safeguard their sensitive PII.

24. This PII includes individuals' account and routing numbers, names, addresses, phone numbers, and check payees and payment amounts.

25. As a custodian of Plaintiff's and Class Members' PII, Alogent assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

26. Despite Defendant's duty to safeguard the PII entrusted to it, Alogent failed to prioritize data protection and cybersecurity by failing to adopt reasonable data and cybersecurity measures to prevent and detect unauthorized access to Plaintiff's and Class Members' PII.

27. Had Alogent remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Alogent could have prevented the intrusion

---

https://www.jdsupra.com/legalnews/alogent-holdings-moveit-data-breach-8361993/ (last visited Dec. 8, 2023).

into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

***B. Defendant Exposed Highly Sensitive Data to Hackers.***

28. Upon information and belief, Alogent engaged Progress Software Corporation to provide it with secure file transfer services—MOVEit.

29. Upon information and belief, in conducting its business, Alogent uses MOVEit, a file transfer software to exchange files with its financial institution clients.

30. Upon information and belief, Alogent maintains MOVEit systems and servers and had control over them at the time of the Data Breach. Alogent stores the PII of its financial institution client's customers on those MOVEit systems and servers.[7]

31. Beginning on or around May 30, 2023, the notorious CL0P ransomware gang exploited a vulnerability in the MOVEit software and accessed, copied, and/or stole Plaintiff's and Class Members' PII stored on Alogent's MOVEit systems and servers.

[7] https://www.doj.nh.gov/consumer/security-breaches/documents/clearwater-credit-union-20230630.pdf (last visited Dec. 8, 2023).

32. The vulnerability allowed CL0P to escalate user privileges and gain unauthorized access to customer environments.[8] Following the discovery of the initial vulnerability in the file transfer software, give additional vulnerabilities were subsequently discovered.[9]

33. However, investigations following CL0P's exploitation of the MOVEit vulnerability have subsequently revealed that CL0P had known about this particular vulnerability and had been experimenting with ways to exploit as far back as 2021.[10]

34. Indeed, one security firm's review of "logs of impacted [MOVEit] clients found evidence of similar [malicious] activity occurring in multiple client environments last year (April 2022) and in some cases as early as July 2021."[11]

---

[8] Matt Kapko, *MOVEit Mass Exploit Timeline: How the File-Transfer Services Attacks Entangled Victims*, CYBERSECURITY DIVE (Sept. 25, 2023), https://www.cybersecuritydive.com/news/moveit-breach-timeline/687417/ (last visited Dec. 8, 2023).

[9] *Id.*

[10] Laurie Iacono et al., *Clop Ransomware Likely Sitting on MOVEit Transfer Vulnerability (CVE-2023-34362) Since 2021*, KROLL (June 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362 (last visited Dec. 8, 2023).

[11] Sergiu Gatlan, *Clop Ransomware Likely Testing MOVEit Zero-Day Since 2021*, BLEEPING COMPUTER (June 8, 2023), https://www.bleepingcomputer.com/news/security/clop-ransomware-likely-testing-moveit-zero-day-since-2021/ (last visited Dec. 8, 2023).

35. The security firm "also discovered the threat actors were testing ways to collect and extract sensitive data from compromised MOVEit Transfer servers as far back as April 2022, likely with the help of automated tools."[12]

36. As such, the 2022 activity and "[t]he malicious activity appeared to be aimed at exfiltrating Organization IDs ("Org IDs") which identified specific MOVEit Transfer users and would have helped Clop determine which organizations it could access."[13]

37. According to Alogent, the Data Breach exposed data contained on a MOVEit server, which included individuals' names, addresses, phone numbers, bank account and routing numbers, and check payees and remittance amounts.[14]

38. Despite the Data Breach occurring between May 30 and June 1, 2023, Alogent did not begin notifying impacted individuals until on or about August 14, 2023, over two months after the Data Breach occurred.[15]

39. Based on Alogent's representations, approximately 4,543,850 individuals' PII was compromised in the Data Breach.[16]

---

[12] *Id.*
[13] Simon Hendery, *Ransomware Gang Clop Prepped Zero-Day MOVEit Attacks in 2021*, SC MAGAZINE (June 9, 2023), https://www.scmagazine.com/news/ransomware-gang-clop-zero-day-moveit-2021 (last visited Dec. 8, 2023).
[14] *Data Breach Notifications – Alogent*, *supra* note 1.
[15] *Id.*
[16] *Id.*

40. Upon information and belief, Class Members received similar Data Breach notices on or around the same time, informing them that their PII was exposed during the Data Breach.

41. The Data Breach occurred as a direct result of Alogent's failure to implement and follow basic data security procedures in order to protect individuals' PII. Alogent could have prevented the Data Breach, or substantially mitigated its severity, if it had properly screened its vendors or contractors, such as Progress Software, for cybersecurity standards as well as conducting cybersecurity audits of its contractors and vendors.

### *C. The Data Breach was a Foreseeable Risk of which Defendant Was on Notice.*

42. Alogent was well aware that the protected PII it acquires is highly sensitive and of significant value to those who would use it for wrongful purposes.

43. Alogent also knew that a breach of its systems or servers, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

44. These risks are not theoretical, numerous high-profile breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, Anthem, Acellion, and Fortra.

45. PII is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including

identity theft, and medical and financial fraud.[17] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

46. The ramifications of Alogent's failure to keep Plaintiff and Class Members' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

47. Further, criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

48. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[18]

[17] *What To Know About Identity Theft*, Fed. Trade Comm'n Consumer Advice (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Dec. 8, 2023).

[18] *Data Breach Report: 2021 Year End*, RISK BASED SEC. (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/ (last visited Dec. 8, 2023).

49. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[19]

50. The financial sector is also a prime target for threat actors. Between January 2018 and September 2023, financial companies have suffered 2,260 data breaches, impacting over 232 million records.[20]

51. The financial sector is "disproportionately targeted by threat actors" because of a simple rational: "[t]hreat actors target organizations that have what they want and what pays big – data and money. Data can be sold for money and vulnerabilities that enable access to both data and money."[21]

52. Indeed, "[h]acking financial organizations can potentially allow malicious threat actors to access accounts or personal information that can help a

[19] *Facts + Statistics: Identity theft and cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports%202015-2019%20 (last visited Dec. 8, 2023).

[20] https://www.comparitech.com/blog/vpn-privacy/financial-data-breaches/#:~:text=2%2C260%20financial%20data%20breaches%20from,over%20101%20million%20in%20total (last visited Dec. 8, 2023).

[21] https://www.paloaltonetworks.com/blog/2021/08/financial-services-cyberattacks/ (last visited Dec. 8, 2023).

criminal gain unauthorized access and make financial transactions or trick others into revealing more information and sending them money."[22]

53. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves the customers of Alogent's financial institution clients especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

54. **Bank Account Numbers and Routing Numbers**—stolen financial account information can have a devastating impact on consumers. Cybercriminals can deplete and wipe out a person's life savings with the click of a button, using an individual's bank account number and routing number to make unauthorized purchases, withdrawals, or transfers.[23]

55. Cybercriminals can sell also bank account information on the dark web between $100 and $3,000 per account. The value of the account information is directly tied to the amount of money in the bank account. Indeed, cybercriminals typically "mention[] the balance on that account along with the victim's physical address. This can be done to hint at the target's potential level of wealth, a toney

[22] https://www.upguard.com/blog/finance-sector-cyber-attacks#:~:text=Hacking%20financial%20organizations%20can%20potentially,information%20and%20sending%20them%20money (last visited Dec. 8, 2023).

[23] https://www.identityguard.com/news/what-information-do-cyber-criminals-steal#:~:text=When%20cybercriminals%20steal%20financial%20information,Ruin%20your%20credit%20reputation (last visited Dec. 8, 2023).

address in Los Angeles or New York City might garner more interest from a buyer."[24]

56. Even if stolen, PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

57. In light of high-profile data breaches at other companies and the value of the PII it stored and collected, Alogent knew or should have known, the importance of safeguarding the PII with which it was entrusted and of the foreseeable consequences if its data security systems were breached. Alogent failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

### *D. Defendant Failed to Comply with FTC Guidelines and Industry Best Practices.*

58. Alogent is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or

[24] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-price-cybercriminals-charge-for-stolen-data/ (last visited Dec. 8, 2023).

affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

59. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[25]

60. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[26]

61. The FTC recommends that businesses:

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

[25] *Start with Security: A Guide for Business*, Fed. Trade Comm'n (June 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Dec. 8, 2023).
[26] *See supra* note 11.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an

attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the

FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. Upon information and belief, Alogent failed to implement one or more of the basic data security practices recommended by the FTC. Alogent's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII—including Plaintiff's and Class Members' names, addresses, phone numbers, and bank account information—constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

64. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[27]

65. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[28] Alogent failed to adhere to the NIST guidance.

---

[27] *See Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, available at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (last visited Dec. 8, 2023).

[28] *Id.* at Table 2 pg. 26-43.

66. Further, cybersecurity experts have identified various best practices that should be implemented by entities in the financial industry, including the following:

a. Regularly assessing risks and auditing cybersecurity;

b. Establishing a cybersecurity policy;

c. Appointing a data protection officer;

d. Securing networks

e. Verifying user identities;

f. Establishing secure password management;

g. Continuously monitor user activity; and

h. Manage third-party risks.[29]

67. Upon information and belief, Alogent's failure to protect Plaintiff's and Class Members' PII is a result of its failure to adopt reasonable safeguards as required by the FTC, NIST, and industry best practices.

68. Alogent was at all times fully aware of its obligations to protect the PII of consumers because of its business model of collecting PII and storing payment information. Alogent was also aware of the significant repercussions that would result from its failure to do so.

[29] https://www.ekransystem.com/en/blog/banking-and-financial-cyber-security-compliance (last visited Dec. 8, 2023).

### *E. Plaintiff and Members of the Class Have Suffered Concrete Injury as a Result of Alogent's Inadequate Security.*

69. The ramifications of Alogent's failure to keep PII secure are long-lasting and severe. Alogent's conduct which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways, including actual fraud as well as substantial and imminent risk of identity theft and fraud. Plaintiff and Class Members must immediately devote time, energy, and money to: (1) closely monitor their bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering, spear phishing, or extortion attacks; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

70. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.[30] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps data breach victims (like

[30] Government Accountability Off., "Data Breaches" (Mar. 2019) https://www.gao.gov/assets/gao-19-230.pdf (last visited Dec. 8, 2023).

Plaintiff and Class Members) must take after a Data Breach like Alogent's are both time-consuming and of only limited and short-term effectiveness.

71. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[31]

72. Further, once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse.

73. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when SPI is stolen and when it is used. According to the GAO, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[32]

---

[31] *See* Identity Theft Victim Checklist, Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last visited Dec. 8, 2023).
[32] *See* 2007 GAO Report, at 29.

74. For these reasons, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Alogent's conduct. Further, the value of Plaintiff's and Class Members' PII has been diminished by its exposure in the Data Breach.

75. Indeed, PII is a valuable commodity to identity thieves, and, once it has been compromised, criminals will use them and trade the information on the cyber black market for years thereafter.[33]

76. The reality is that cybercriminals seek nefarious outcomes from a data breach and stolen PII can be used to carry out a variety of crimes.

77. Plaintiff and Class Members are also at a continued risk because their information remains in Alogent's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Alogent fails to undertake the necessary and appropriate security and training measures to protect its customers' PII.

78. As a result of Alogent's failures, Plaintiff and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of

[33] *The Price Cybercriminals Charge for Stolen Data*, Trustwave (Aug. 6, 2023), https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-price-cybercriminals-charge-for-stolen-data/ (last visited Dec. 8, 2023).

the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

79. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information to strangers and cybercriminals.

### *F. Plaintiff's Experience*

80. Plaintiff is customer of one of Alogent's financial institution clients. Plaintiff provided her PII to Alogent as part of Alogent's check processing services. When providing her PII to Alogent, Plaintiff reasonably expected that Alogent would implement adequate data security measures to safeguard her PII.

81. On or about [insert, 2023], Plaintiff received a letter from Alogent informing her that her PII in Defendant's possession had been compromised in the Data Breach.

82. While Defendant has provided Plaintiff with an offer of credit monitoring, this offer is time-limited and will expire long before the threat to Plaintiff's PII. And in any event, Alogent puts the onus on Plaintiff to protect her PII suggesting that she watch for suspicious activity.

83. Plaintiff has suffered actual injury from having her PII exposed and/or stolen as a result of the Data Breach, including: (1) required mitigation efforts, including needing to monitor her financial accounts to ensure her information is not

used for identity theft and fraud; (b) damages to and diminution of the value of her PII, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; (c) loss of privacy; and (d) continuous imminent and impending injury raising from increased risk of financial, medical, and identity theft and fraud.

84. As a result of the Data Breach Plaintiff has spent her valuable time and effort to mitigate any future misuse of her PII compromised in the Data Breach. These efforts include spending approximately three to five hours a week monitoring her financial accounts, spending time to change her passwords to her financial accounts, and spending two to three hours investigating dark web monitoring alerts she received after the Data Breach.

85. In addition, knowing that hackers accessed and likely exfiltrated her PII and that this information likely has been and will be used in the future for identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

86. As a direct and proximate result of the Data Breach, Plaintiff has been and will continue to be at a heightened risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending,

and is not speculative, given the highly sensitive nature of the PII compromised in the Data Breach.

## CLASS ALLEGATIONS

87. Plaintiff brings this action on behalf of herself and all other similarly situated Class Members pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure.

88. Plaintiff seeks to represent a class of person to be defined as follows:

> All individuals in the United States and its territories whose PII was compromised during the Data Breach, which was announced on or about August 14, 2023 (the "Class").

89. Excluded from the class are Defendant and its subsidiaries and affiliates; all employees of Defendant; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

90. Plaintiff reserves the right to, after conducting discovery, modify, expand, or amend the above Class definition or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate.

91. **Numerosity**. Plaintiff is informed and believes, and thereon alleges, that there are, at minimum, millions of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable

through Alogent's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 4.5 million individuals.

92. **Commonality and Predominance**. This action involves questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Alogent had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Alogent was negligent in collecting and storing Plaintiff's and Class Members' PII, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Alogent's wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Alogent's wrongful conduct.

93. **Typicality**. Plaintiff's claims are typical of the claims of the members of the Class. The claims of Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Alogent was the custodian of Plaintiff's and Class Members' PII, when their PII was obtained by an unauthorized third party.

94. **Adequacy**. Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendant to obtain relief for herself and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel that is competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

95. **Superiority**. Class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit financial institutions to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

96. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical

violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Alogent's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

97. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

98. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Alogent's books and records.

**FIRST CAUSE OF ACTION**
**NEGLIGENCE**
**(On Behalf of Plaintiff and the Class)**

99. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 through 98 as if fully set forth herein.

100. Alogent owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding,

deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons.

101. Alogent's duty to use reasonable care arose from several sources, including but not limited to those described below.

102. Alogent had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate data security practices on the part of Defendant. By receiving, maintaining, and handling PII that is routinely targeted by criminals for unauthorized access, Alogent was obligated to act with reasonable care to protect against these foreseeable threats.

103. Alogent also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiff and Class Members. Alogent's conduct included its failure to adequately restrict access to its computer networks and/or servers that held individuals' PII.

104. Alogent also knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing adequate data security measures to protect that PII, and the frequency of cyberattacks such as the Data Breach in the financial sector.

67. Alogent is subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and Defendant and Class Members. The sources of Alogent's duty are identified above.

105. Alogent's duty included, among other things: (a) designing, maintaining, and testing Alogent's security systems to ensure that Plaintiff's and Class Members' PII in Alogent's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warning and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

106. Upon information and belief, Alogent alone controlled its technology, infrastructure, and cybersecurity. Alogent further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, Alogent knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen.

107. Alogent breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and

external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies provided to its customers; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

108. But for Alogent's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not be compromised.

109. As a direct and proximate result of Alogent's negligence, Plaintiff and the Class have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Time spent addressing and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach;

g. Costs associated with the time spent addressing and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach;

h. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

i. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Alogent with the mutual understanding that Alogent would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

j. Continued risk of exposure to hackers and thieves of their PII, which remains in Alogent's possession and is subject to further

breaches so long as Alogent fails to undertake appropriate and adequate measures to protected Plaintiff.

110. As a direct and proximate result of Alogent's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

**SECOND CAUSE OF ACTION**
**NEGLIGENCE *PER SE***
**(On Behalf of Plaintiff and the Class)**

111. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 through 98 as if fully set forth herein.

112. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Alogent for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Alogent's duty.

113. Alogent violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and not complying with the industry standards. Alogent's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

114. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

115. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

116. Alogent's violation of Section 5 of the FTC Act constitutes negligence *per se*.

117. As a direct and proximate result of Alogent's negligence, Plaintiff and Class Members have suffered injuries, including those identified in paragraph 109 above.

118. As a direct and proximate result of Alogent's negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

**THIRD CAUSE OF ACTION**
**DECLARATORY JUDGMENT**
**(On Behalf of Plaintiff and the Class)**

119. Plaintiff repeats and re-alleges the allegations contained paragraphs 1 through 98 as if fully set forth herein.

120. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described herein.

121. Alogent owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' PII.

122. Alogent still possesses PII regarding Plaintiff and Class Members.

123. An actual controversy has a risen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Alogent is currently maintaining data security measures to protect Plaintiff and Class members from further data breaches that compromise their PII. Plaintiff alleges that Alogent's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and the risk remains that further compromises of their PII will occur in the future, especially in light of Alogent's recent history of data breaches.

124. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Alogent owes a legal duty to secure consumers' PII under the common law and Section 5 of the FTC Act; and

b. Alogent continues to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiff's and Class Members' PII.

125. This Court also should issue corresponding prospective injunctive relief requiring Alogent to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

126. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Alogent. The risk of another such breach is real, immediate, and substantial. If another breach at Alogent occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

127. The hardship to Plaintiff and Class members if an injunction is not issued exceeds the hardship to Alogent if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Alogent of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Alogent has a pre-existing legal obligation to employ such measures.

128. Issuance of the requested injunction will not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach at Alogent, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and,

H. Awarding such other and further relief as may be just and proper.

**JURY TRIAL DEMAND**

A jury trial is demanded on all claims so triable.

Dated: December 12, 2023

Respectfully submitted,

*/s/ Nicholas A. Colella*
Gary F. Lynch*
Nicholas A. Colella
(Ga. Bar No. 299972)
**LYNCH CARPENTER LLP**
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com
nickc@lcllp.com

Joseph P. Guglielmo*
**SCOTT+SCOTT**
**ATTORNEYS AT LAW LLP**
230 Park Avenue, 17th Floor
New York, NY 10169
(212) 223-6444
jguglielmo@scott-scott.com

Brian C. Gudmundson*
**ZIMMERMAN REED LLP**
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com

Andrea R. Gold*
**TYCKO & ZAVAREEI LLP**
2000 Pennsylvania Avenue NW #1010
Washington, DC 20006
(202) 973-0900
agold@tzlegal.com

**pro hac vice forthcoming*

*Attorneys for Plaintiff and the Proposed Class*